1120.41193X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: T. PIRTTIMAA, et al

Serial No.: Not assigned

Filed: February 13, 2002

For: METHOD AND NETWORK ELEMENT FOR PROVIDING SECURE ACCESS TO A PACKET DATA NETWORK

Group: Not assigned

Examiner: Not assigned

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

February 13, 2002

Sir:

Prior to examination, please amend the above-identified application as follows.

IN THE CLAIMS

Please amend the claims as follows:

1. (Amended) A method for providing secure access to a packet data network, said method comprising:

a) receiving a message from a terminal device , connected to said packet data network;

b) deriving a first source information from said message;

c) deriving a second source information;

d) comparing said first and second source information; and

e) initiating a protection processing based on the result of said comparing step.

3. (Amended) A method according to claim 1, wherein said second source information is a source address information derived from a packet data unit used for conveying said message, or from a security association set up between said terminal device and said packet data network.

4. (Amended) A method according to claim 1, wherein said protection processing comprises a processing for dropping said message if said comparing step leads to the result that said first source information and said second source information do not indicate the same location.

5. (Amended) A method according to claim 1, wherein said protection processing comprises a processing for dropping said message if said comparing step leads to the result that said first source information and said second source information do not match.

6. (Amended) A method according to claim 1, wherein said first source information is an IP address.

8. (Amended) A method according to claim 1, wherein said second source information is at least a part of an IP source address of an IP datagram.

12. (Amended) A method according to claim 10, wherein said message is conveyed using a SIP-level protection function.

13. (Amended) A network element for providing secure access to a packet data network, said network element comprising:

a) receiving means for receiving a message from a terminal device connected to said network element ;

b) deriving means for deriving a first source information from said message, and for deriving a second source information;

c) comparing means for comparing said first and second source information; and

d) protecting means for initiating a protection processing based on the comparing result of said comparing means.

14. (Amended) A network element according to claim 13, wherein said deriving means is arranged for deriving said second source information from a packet data unit used for conveying said message or from a security association set up between said terminal device and said network element .

15. (Amended) A network element according to claim 13, wherein said deriving means is arranged for deriving said first source information from a header portion of said message.

16. (Amended) A network element according to any one of claims 13, wherein said protecting means are arranged to initiate a processing for dropping said message if said comparing result indicates that said first source information and said second source

information do not indicate the same location.

17. (Amended) A network element according to any one of claims 13, wherein said protecting means are arranged to initiate a processing for dropping said message if said comparing result indicates that said first source information and said second source information do not match.

18. (Amended) A network element according to any one of claims 13, wherein said deriving means are arranged for reading said second source information from a database provided at said network element.

19. (Amended) A network element according to any one of claims 13, wherein said deriving means are arranged for deriving said second source information by extracting an IP source address from an IP datagram.

20. (Amended) A network element according to any one of claims 13, wherein said network element is a proxy server.

21. (Amended) A network element according to claim 20, wherein said proxy server is a P-CSCF of an IP Mobility Subsystem.

Please add new claims 22-35 as follows:

-- 22. A method according to claim 2, wherein said second source information is a source address information derived from a packet data unit used for conveying said message, or from a security association set up between said terminal device and said packet data

network.

23. A method according to claim 22, wherein said protection processing comprises a processing for dropping said message if said comparing step leads to the result that said first source information and said second source information do not indicate the same location.

24. A method according to claim 23, wherein said protection processing comprises a processing for dropping said message if said comparing step leads to the result that said first source information and said second source information do not match.

25. A method according to claim 24, wherein said first source information is an IP address.

26. A method according to claim 25, wherein said message is a SIP message.

27. A method according to claim 26, wherein said second source information is at least a part of an IP source address of an IP datagram.

28. A method according to claim 11, wherein said message is conveyed using a SIP-level protection function.

29. A network element according to claim 14, wherein said deriving means is arranged for deriving said first source information from a header portion of said message.

30. A network element according to any one of claims 29, wherein said protecting means are arranged to initiate a processing for dropping said message if said comparing result indicates that said first source information and said second source information do not indicate the same location.

31. A network element according to any one of claims 30, wherein said protecting means are arranged to initiate a processing for dropping said message if said comparing result indicates that said first source information and said second source information do not match.

32. A network element according to any one of claims 31, wherein said deriving means are arranged for reading said second source information from a database provided at said network element.

33. A network element according to any one of claims 32, wherein said deriving means are arranged for deriving said second source information by extracting an IP source address from an IP datagram.

34. A network element according to any one of claims 33, wherein said network element is a proxy server.

35. (Amended) A network element according to claim 34, wherein said proxy server is a P-CSCF of an IP Mobility Subsystem. --

REMARKS

Attached hereto is a marked-up version of the changes made to the claims by the current Amendment. The attached page is captioned "**Version with markings to show changes made**".

Please charge any shortage in fees due in connection with the filing of this paper, or credit any overpayment of fees, to the deposit account of Antonelli, Terry, Stout & Kraus, LLP, Deposit Account No. 01-2135 (1120.41193X00).

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Carl I. Brundidge
Registration No. 29,621

CIB/jdc
(703) 312-6600

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE CLAIMS

Please amend the claims as follows:

2. (Amended) A method for providing secure access to a packet data network, said method comprising:

f) receiving a message from a terminal device ~~(40, 60)~~, connected to said packet data network;

g) deriving a first source information from said message;

h) deriving a second source information;

i) comparing said first and second source information; and

j) initiating a protection processing based on the result of said comparing step.

3. (Amended) A method according to claim 1 ~~or 2~~, wherein said second source information is a source address information derived from a packet data unit used for conveying said message, or from a security association set up between said terminal device ~~(40, 60)~~ and said packet data network.

4. (Amended) A method according to claim 1 ~~any one of the preceding claims~~, wherein said protection processing comprises a processing for dropping said message if said comparing step leads to the result that said first source information and said second source information do not indicate the same location.

5. (Amended) A method according to claim 1 ~~any one of the preceding claims~~,

wherein said protection processing comprises a processing for dropping said message if said comparing step leads to the result that said first source information and said second source information do not match.

6. (Amended) A method according to claim 1 ~~any one of the preceding claims~~, wherein said first source information is an IP address.

9. (Amended) A method according to claim 1 ~~any one of the preceding claims~~, wherein said second source information is at least a part of an IP source address of an IP datagram.

12. (Amended) A method according to claim 10 ~~or 11~~, wherein said message is conveyed using a SIP-level protection function.

13. (Amended) A network element for providing secure access to a packet data network, said network element ~~(30)~~ comprising:

~~a)~~e) receiving means ~~(31)~~ for receiving a message from a terminal device ~~(40, 60)~~ connected to said network element ~~(30)~~;

~~b)~~f) deriving means ~~(31)~~ for deriving a first source information from said message, and for deriving a second source information;

~~c)~~g) comparing means ~~(33)~~ for comparing said first and second source information; and

h) protecting means ~~(32)~~ for initiating a protection processing based on the comparing result of said comparing means.

14. (Amended) A network element according to claim 13, wherein said

deriving means ~~(31)~~ is arranged for deriving said second source information from a packet data unit used for conveying said message or from a security association set up between said terminal device ~~(40, 60)~~ and said network element ~~(30)~~.

15. (Amended) A network element according to claim 13 ~~or 14~~, wherein said deriving means ~~(31)~~ is arranged for deriving said first source information from a header portion of said message.

16. (Amended) A network element according to any one of claims 13 ~~to 15~~, wherein said protecting means ~~(32)~~ are arranged to initiate a processing for dropping said message if said comparing result indicates that said first source information and said second source information do not indicate the same location.

17. (Amended) A network element according to any one of claims 13 ~~to 15~~, wherein said protecting means ~~(32)~~ are arranged to initiate a processing for dropping said message if said comparing result indicates that said first source information and said second source information do not match.

18. (Amended) A network element according to any one of claims 13 ~~to 17~~, wherein said deriving means are arranged for reading said second source information from a database ~~(34)~~ provided at said network element.

19. (Amended) A network element according to any one of claims 13 ~~to 18~~, wherein said deriving means ~~(31)~~ are arranged for deriving said second source information by extracting an IP source address from an IP datagram.

20. (Amended) A network element according to any one of claims 13 ~~to 19~~, wherein said network element is a proxy server ~~(30)~~.

21. (Amended) A network element according to claim 20, wherein said proxy server is a P-CSCF ~~(30)~~ of an IP Mobility Subsystem.